



# ISBA Mutual Mirza Risk Management Conference

Collinsville, IL

May 14, 2024

# Table of Contents

Anatomy of an ARDC / Legal Malpractice Claim	3
Anatomy of a Lawyers Professional Liability Policy	24
Ethical and Business Considerations in Choosing IT Services	44
IT Vendor Assessment Worksheet	73



# Anatomy of an ARDC/Legal Malpractice Claim

Amanda Hamilton  
Konicek & Dillon, P.C.



## What is Legal Malpractice?

- ▶ “The law does not say how a reasonably careful lawyer would act under these circumstances. That is for you to decide. In reaching your decision, you must rely upon opinion testimony from qualified witnesses [and evidence of the Rules of Professional Conduct]. You must not attempt to determine how a reasonably careful lawyer would act from any personal knowledge you may have.” – IPI 105.01

# Elements

Duty

Breach

Proximate Cause

Actual Damages

# Duty

---

“A lawyer must possess and use the knowledge, skill, and care ordinarily used by a reasonably careful lawyer.”  
IPI 105.01

---

Comply with the Illinois Rules of Professional Conduct

# Duty

## Consensual Relationship

- Acceptance from attorney
- Authority from client

## Type of Representation Sought

## Scope of Authority Conferred

# Breach

- ▶ “A lawyer must possess and use the knowledge, skill, and care ordinarily used by a reasonably careful lawyer. The failure to do something that a reasonably careful lawyer would do, under circumstances similar to those shown by the evidence, is ‘professional negligence.’”
- ▶ “The phrase ‘deviation from the standard of care’ means the same thing as ‘professional negligence.’”  
IPI 105.01
- ▶ Generally, expert testimony required
  - ▶ Exceptions





# Proximate Cause

## Litigation

- ▶ The “case within a case”
- ▶ Compensated by some third party “but for” the acts/omissions of the attorney
  - ▶ Governmental Interinsurance Exchange v. Judge, 221 Ill.2d 195 (2006)

## Transaction

- ▶ “Client’s exposure to a risk that the client did not knowingly and voluntarily assume.”
  - ▶ Union Planters Bank, N.A. v. Thompson Coburn, LLP, 402 Ill.App.3d 317 (5th Dist. 2010)

# Actual Damages

Actually  
incurred

Specific to  
Plaintiff

Attorney's  
Fees

Punitive  
Damages

Pre-judgment  
interest

"Same  
position"

# Applicable statutes of limitation and repose – General Rules

- ▶ § 13-214.3. Attorneys.
- ▶ (b) An action for damages based on tort, contract, or otherwise (i) against an attorney arising out of an act or omission in the performance of professional services or (ii) against a non-attorney employee arising out of an act or omission in the course of his or her employment by an attorney to assist the attorney in performing professional services must be commenced within 2 years from the time the person bringing the action knew or reasonably should have known of the injury for which damages are sought.
- ▶ (c) Except as provided in subsection (d), an action described in subsection (b) may not be commenced in any event more than 6 years after the date on which the act or omission occurred.

# Applicable statutes of limitation and repose - Exceptions

- ▶ (d) When the injury caused by the act or omission does not occur until the death of the person for whom the professional services were rendered, the action may be commenced within 2 years after the date of the person's death unless letters of office are issued or the person's will is admitted to probate within that 2 year period, in which case the action must be commenced within the time for filing claims against the estate or a petition contesting the validity of the will of the deceased person, whichever is later, as provided in the Probate Act of 1975. An action may not be commenced in any event more than 6 years after the date the professional services were performed.
- ▶ (e) If the person entitled to bring the action is under the age of majority or under other legal disability at the time the cause of action accrues, the period of limitations shall not begin to run until majority is attained or the disability is removed.
- ▶ (f) If the person entitled to bring an action described in this Section is not under a legal disability at the time the cause of action accrues, but becomes under a legal disability before the period of limitations otherwise runs, the period of limitations is stayed until the disability is removed. This subsection (f) does not invalidate any statute of repose provisions contained in this Section. This subsection (f) applies to actions commenced or pending on or after January 1, 2015 (the effective date of Public Act 98-1077).

# ...but do not forget equitable estoppel and fraudulent concealment

- ▶ Misrepresent or conceal material facts
  - ▶ Knowledge that the representations were untrue
  - ▶ Lack of knowledge by receiving party at time of receipt and action
  - ▶ Intention for receiving party to reasonably rely
  - ▶ Action in good faith to his/her detriment
  - ▶ Prejudice
  - ▶ Brummel v. Grossman, 2018 IL App (1st) 162540
  - ▶ Concealed a material fact under circumstances which created a duty to speak
  - ▶ Defendant intended to induce a false belief
  - ▶ Plaintiff could not have discovered the truth through reasonable inquiry or inspection (or was prevented from doing so)
  - ▶ Justifiable reliance on silence
- Abazari v. Rosalind Franklin University of Medicine and Science, 2015 IL App (2d) 140952

# Attorneys as fiduciaries

- ▶ “A fiduciary relationship exists as a matter of law between an attorney and his client. Thus, in effect any alleged malpractice by an attorney also evidences a simultaneous breach of trust; however, that does not mean every cause of action for professional negligence also sets forth a separate and independent cause of action for breach of fiduciary duty.” *Brush v. Gilsdorf*, 335 Ill.App.3d 356 (3d Dist. 2002).
- ▶ Pleading in the alternative
- ▶ Damages available
  - ▶ Section 2-1115 prohibits punitive damages for legal malpractice claims

# Attorneys as trustees

- ▶ Illinois Trust and Trustees Act and the Illinois Trust Code
- ▶ Significant changes, including, but not limited to:
  - ▶ The Trustee's (prospective) duty to inform and account (Section 813)
  - ▶ ITC codifies the duty of loyalty (Section 802(c))
  - ▶ Permits a Trustee to delegate certain duties (Section 807)
  - ▶ Limits a Trustee's duties regarding trust-owned life insurance policies if proper notices sent (Section 913)
  - ▶ Exculpation clauses invalid if drafted by Trustee unless "objectively fair and disclosed to settlor" (Section 1008)
  - ▶ Consent, ratification, and release all defenses to claims of breach (Section 1009)



# CIVIL Claim Procedure

Complaint

Motion Practice

Written Discovery

Oral Discovery

213(f)(3) Written and Oral Discovery

Dispositive Motions

Jury Trial

Appellate Court

Supreme Court

# ARDC Complaint Procedure

Grievance

Investigation

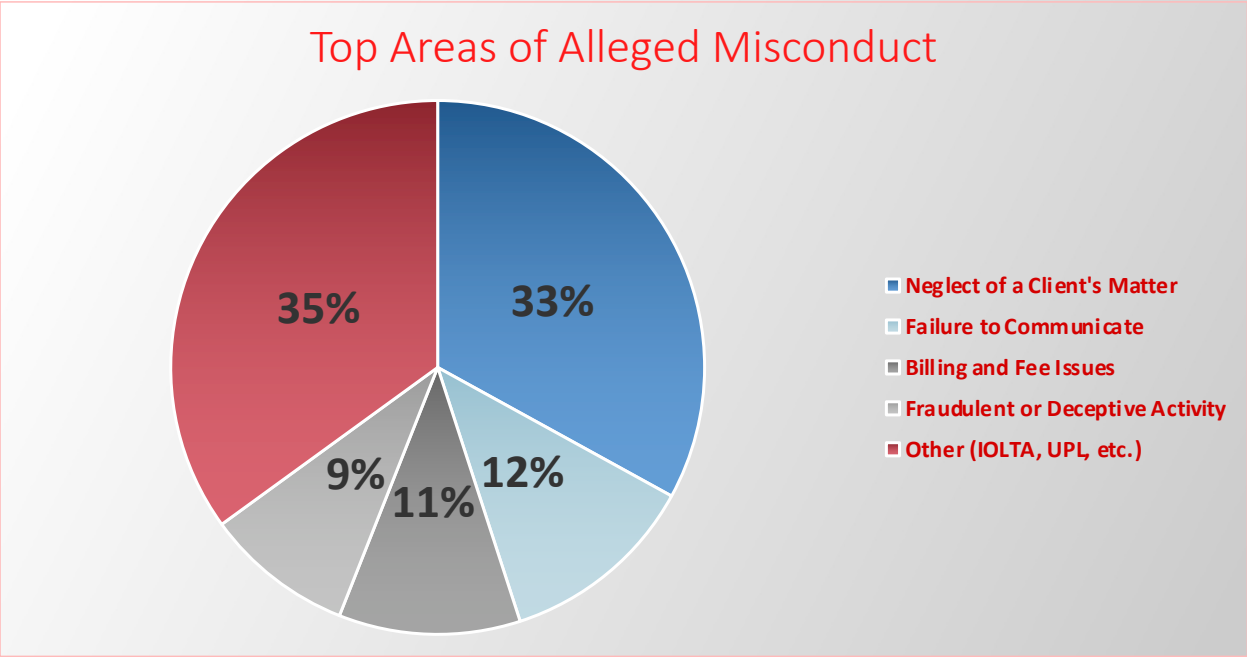
Inquiry Board

Hearing Board

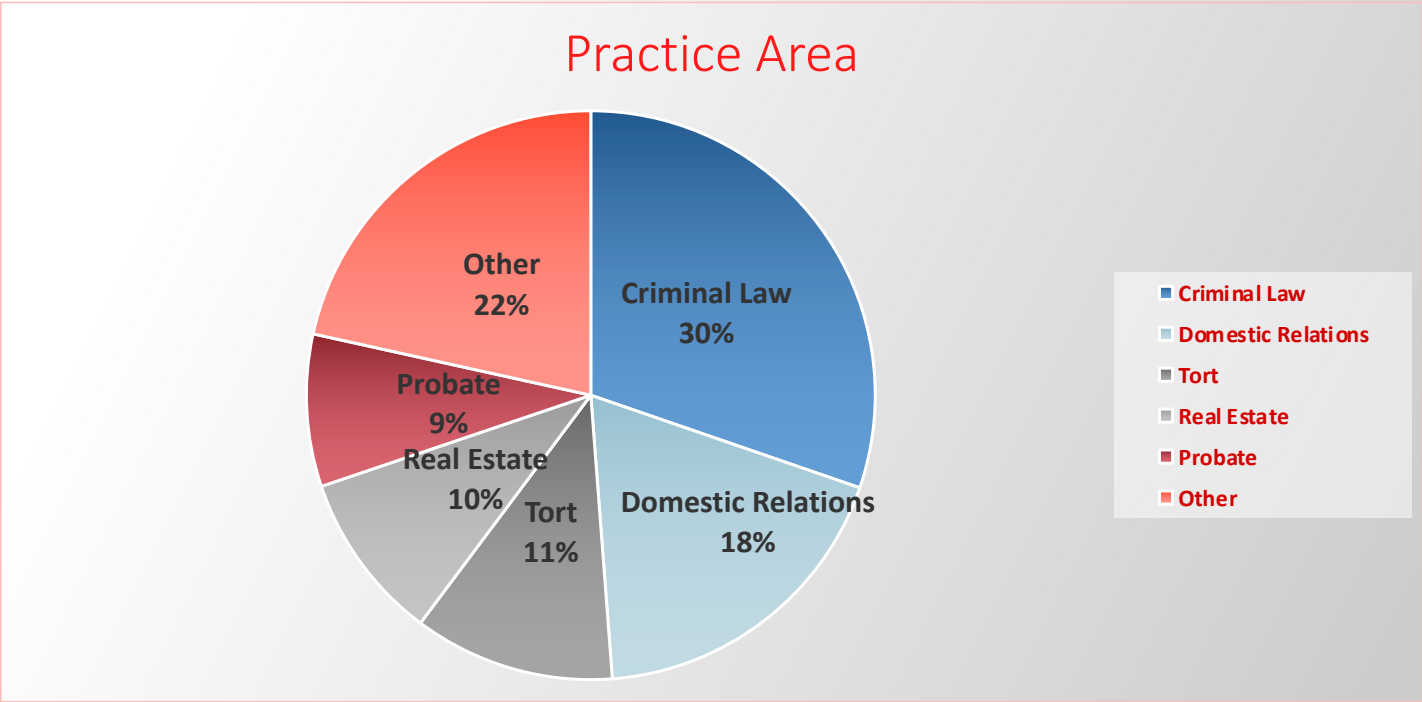
Review Board

Supreme Court

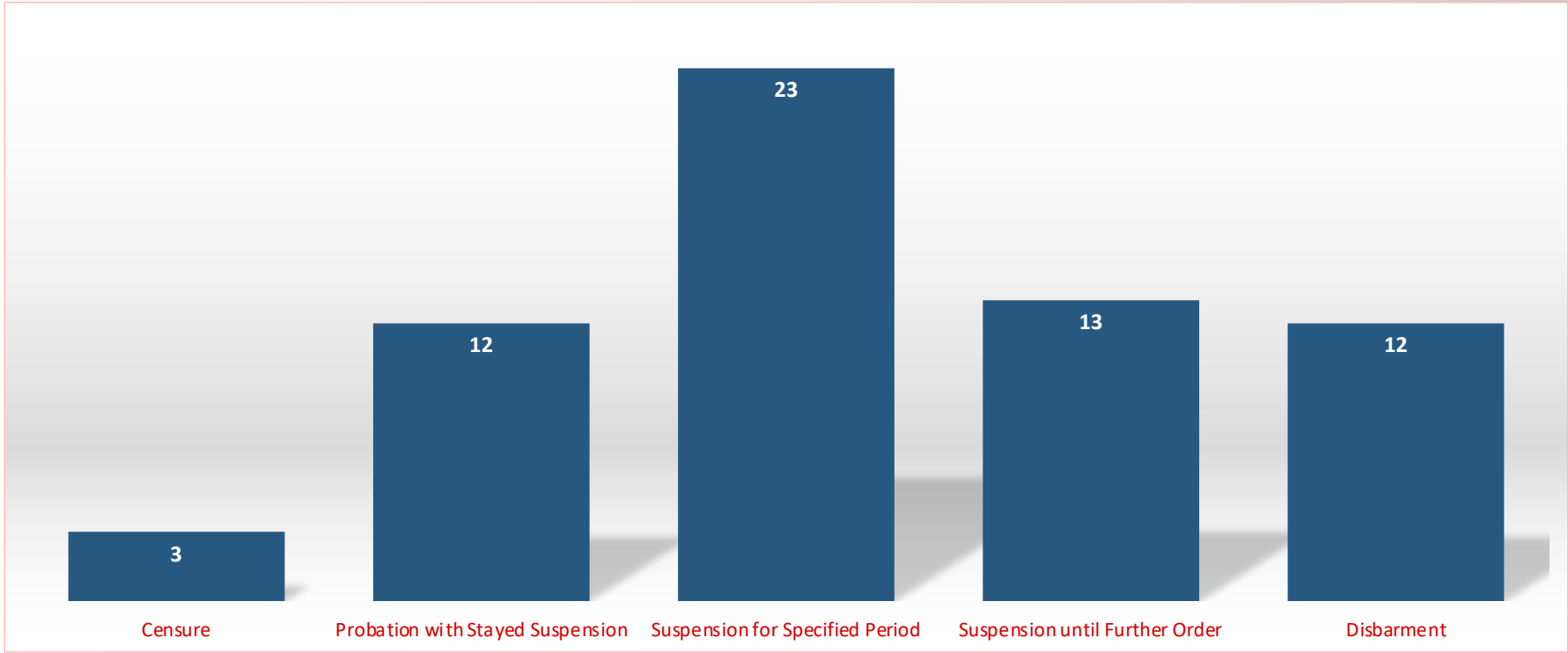
# 2022 ARDC Statistics – Types of Misconduct Alleged in Complaints



# 2022 ARDC Statistics – Practice Areas



# 2022 Types of Discipline



# Takeaway

**DON'T** Procrastinate or Overestimate Expertise

**SEEK** Advice from Counsel and Insurance

**BE** Honest, Conscientious, and Vigilant

**Avoid** Avoid Complacency

# Questions and Discussion



# Anatomy of a Lawyers' Professional Liability Policy

ISBA Mutual Mirza Risk  
Management Conference 2024  
May 14, 2024



# Introduction and Overview



Mosea Harris, CPCU, Sr. Claims and Risk Manager  
ISBA Mutual Insurance Company

Mosea Harris has 30 years experience in Claims, with specific focus on lawyers' professional liability. Mosea has a BA in Economics from Eastern Illinois University and also holds MDiv from Virginia Union University.



Scott Dutton, Chief Relationship Office  
ISBA Mutual Insurance Company

Scott Dutton leads the business unit delivering marketing, communications, education and client/member experience. Scott has over 30 years of insurance industry experience including executive and management roles at both insurance companies and brokerages.

# Today's Structure and Objectives

At the end of this program, you will have a better understanding of the basic components of a lawyer's professional liability insurance policy. You will also learn how an insurance company interprets its own policy language and applies that interpretation to claims handling.

We will also share current professional liability claims trends and examples of some current professional liability claims.

# What is the purpose of a Professional Liability Insurance Policy

- ▶ Protect the Client and the Public
- ▶ Defend the Lawyer/Firm
- ▶ Elevate the Legal Profession



# Components of an Insurance Contract (aka policy)

- ▶ Declarations Page
- ▶ Coverage Agreement
- ▶ Supplementary Coverages
- ▶ Definitions
- ▶ Limit of Liability and Deductible
- ▶ Conditions
- ▶ Exclusions
- ▶ Extended Reporting Period

Source: ISBA Mutual Insurance Company Policy Agreement

# Declaration Page

ISBA Mutual Insurance Company (An Illinois Mutual Insurance Company)

## Lawyers' Professional Liability Policy Declarations

1. Policy Number: 131424-3-2302
2. Named Insured: Emmerth Divorce Law, PLLC
3. Principal Address: 27475 Ferry Road  
Suite 169  
Warrenville, IL 60555
4. Prior Acts Date: 02/01/2021
5. Policy Period: From 02/01/2023 To 02/01/2024  
At 12:01AM CST at address in item 3 of Insured named in Item 2
6. Annual Premium: \$2,669
7. Limit of Liability: Per Claim \$3,000,000 Aggregate \$3,000,000
8. Deductible: Per Claim \$5,000
9. Date of Application: 1/10/2023

### Attached Forms and Endorsements:

- ISBAMIC LPL Policy 01 2023 Policy
- ISBAMIC 102 01 2018 Individual Prior Acts Date Endorsement

This schedule including all endorsements listed herein, is incorporated in and made part of the policy to which it applies.

Source: ISBA Mutual Insurance Company Policy Agreement

# Coverage Agreement

## Claims Made and Reported

### I. COVERAGE AGREEMENTS

- A. The **Company** agrees to pay on the **Insured's** behalf **Claim Expenses** in accordance with the terms of this Policy and all **Damages** in excess of the **Deductible**, up to the Limit of Liability, which the **Insured** becomes legally obligated to pay as a result of a **Claim** first made against an **Insured** and reported to the **Company** in writing during the **Policy Period** or any **Extended Reporting Period**, if applicable, provided that:
1. the **Claim** arises out of a **Wrongful Act** which occurred on or after the **Prior Acts Date** but before the end of the **Policy Period**;
  2. as of the effective date of this Policy, the **Insured** had no knowledge of the **Claim**;
  3. notice of the **Claim** was not given nor required to be given to any prior insurer; and
  4. no **Insured** had a basis to believe any **Wrongful Act** might reasonably be expected to be the basis of a **Claim**.



Source: ISBA Mutual Insurance Company Policy Agreement

# Professional Services

Services rendered by the **Insured** as a Lawyer, whether or not for a fee.



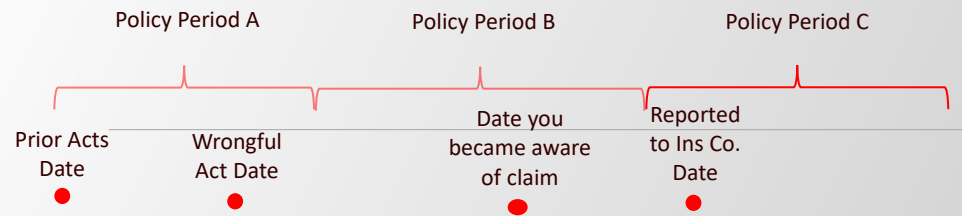
# Supplemental Coverages

- ▶ Loss of earnings
- ▶ ARDC/Disciplinary coverage
- ▶ Cyber Coverage
- ▶ At ISBA Mutual we pay first dollar defense regardless of your deductible





# Coverage Period v Policy Period (claims made policies)

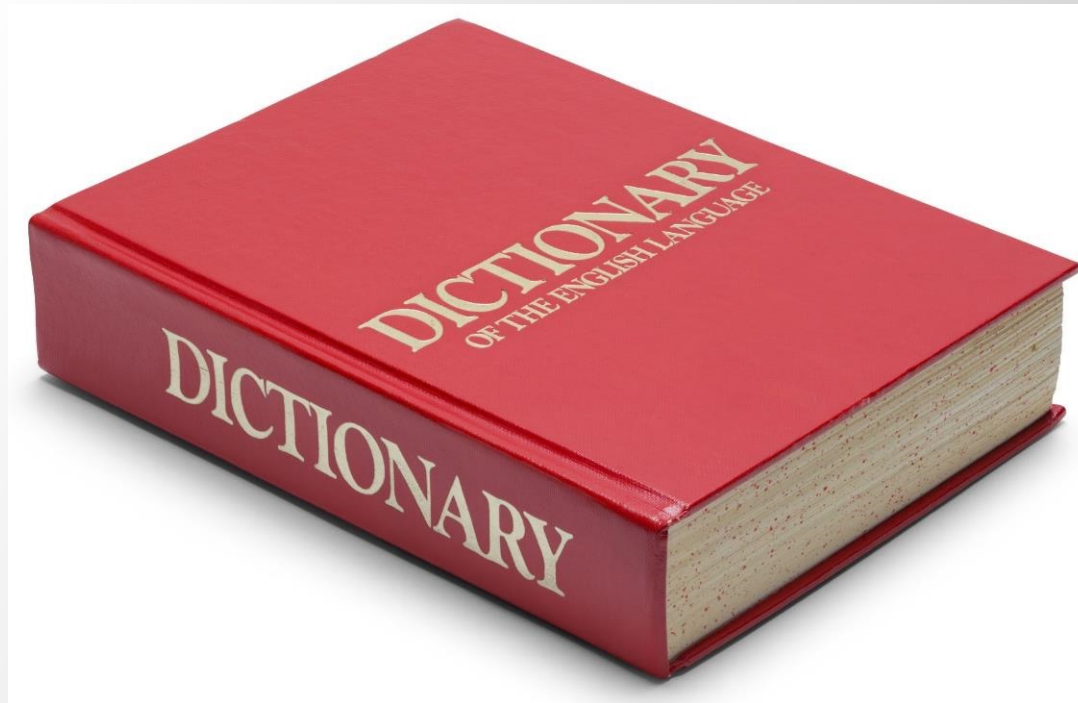


Wrongful Act date: The date when the alleged Wrongful Act took place.

Claim made date: The date a lawyer within the firm became aware of the alleged Wrongful Act.

Report date: The date the firm informs the insurance company of the alleged Wrongful Act.

# Definitions (see Glossary)



# The Named Insured

- ▶ NAMED INSURED is the lawyer or law firm to whom the policy is issued

**Illinois State Bar Association Mutual Insurance Company**  
(An Illinois Mutual Insurance Company)

**Lawyers' Professional Liability Policy Declarations**

2. Named Insured:	World's Best Law Firm
3. Principal Address:	1060 W. Addison Left Field Bleachers Chicago, IL 60613
5. Policy Term:	From May 22, 2018 to May 22, 2019 At 12:01 AM CST at address of Insured named in Item 2
6. Annual Premium:	\$ 1,500.00
7. Limit of Liability:	Per Claim \$1,000,000      Aggregate \$3,000,000
8. Deductible: PerClaim	\$ 5,000
9. Date of Application:	May 22, 2018

Attached Forms and Endorsements:

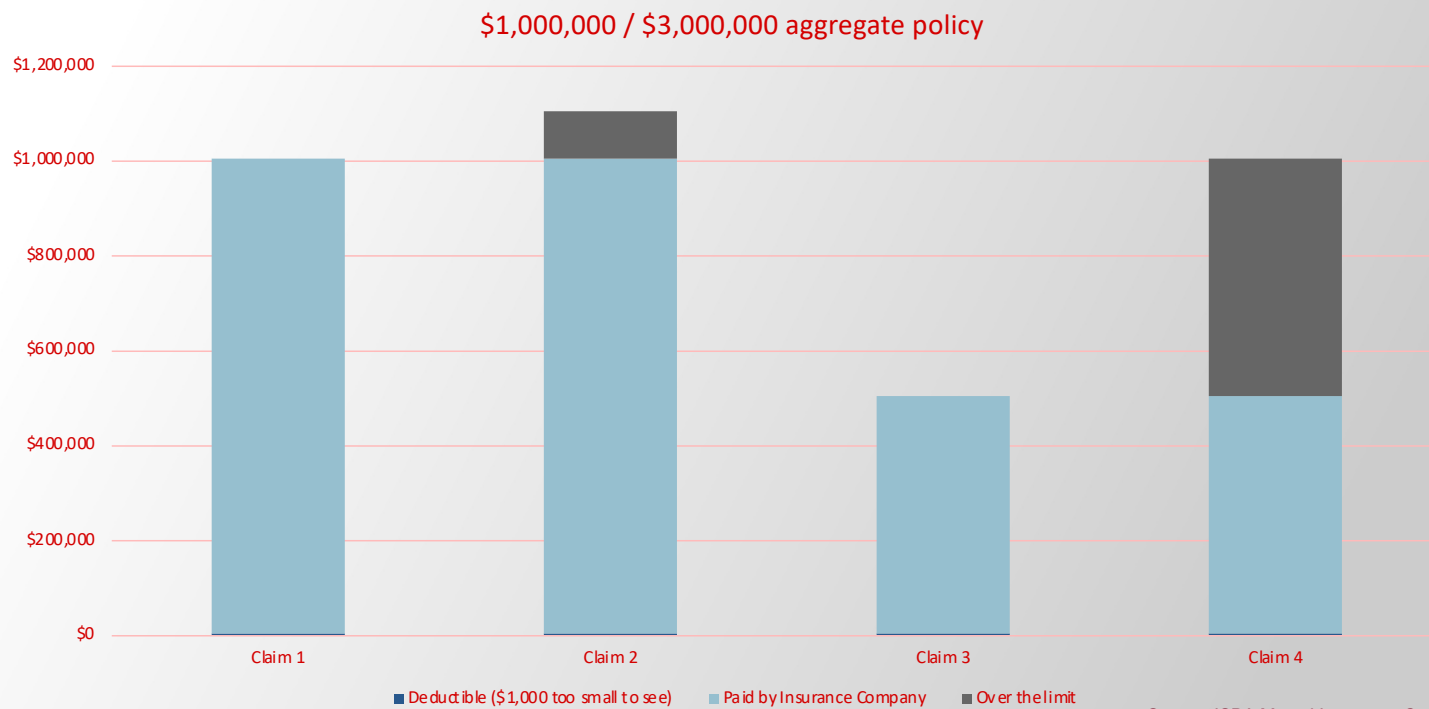
This schedule including all endorsements listed herein, is incorporated in and made part of the policy to which it applies.

Source: ISBA Mutual Insurance Company Policy Agreement

# Claim, Claims Expenses, Damages



# Limits of Liability & Deductible



Source: ISBA Mutual Insurance Company Policy Agreement

# Conditions

- ▶ Application & Supplements: Provide accurate and complete information
- ▶ Timely Notice of Claim
- ▶ Required to notify insurance company of material changes to your firm (new location, new lawyer(s), practicing in another state)
- ▶ Timely payment of Premium and Deductible

# Exclusions

- ▶ Intentional or criminal acts
- ▶ Revoked or suspended license
- ▶ Work as a Public Official / Government Employee
- ▶ Investment advice
- ▶ Outside interests
- ▶ Insured vs. insured
- ▶ Office sharing
- ▶ Beneficiary of a trust

- ▶ Anything covered under another policy



- ▶ Nuclear radiation

Source: ISBA Mutual Insurance Company Policy Agreement

# Extended Reporting Period

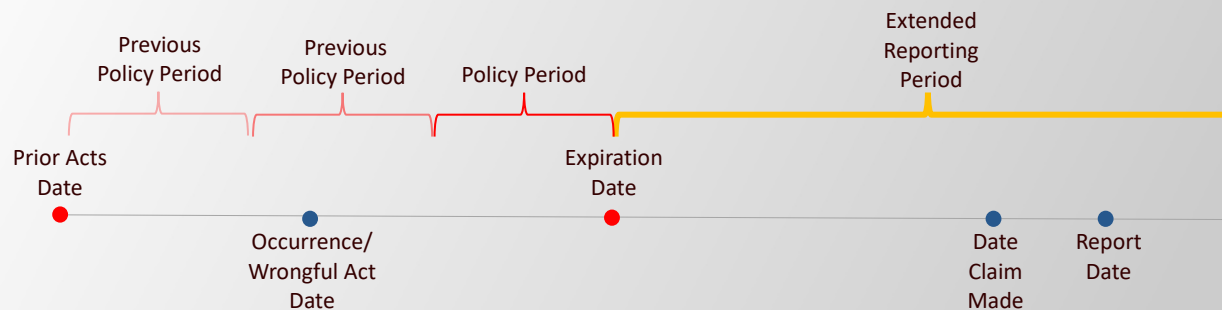
The period of time after the end of the **Policy Period** during which **Claims** may be reported.





# Extended Reporting Period

- ▶ Also known as a “tail”
- ▶ Only covers work during the policy period
- ▶ Types
  - ▶ Optional
  - ▶ Death/disability
  - ▶ Retirement
  - ▶ Military duty
- ▶ You have 60 days to purchase ERP from expiration / cancellation date
- ▶ Must be paid in full, can't be cancelled or renewed



# What a Lawyers Professional Liability Policy is NOT

- ▶ Cyber Liability Insurance
- ▶ General Liability / Business Owners Insurance
- ▶ Workers' Compensation Insurance
- ▶ Business Auto Insurance
- ▶ Business Umbrella Policy



# Thank you!

Questions?



# Ethical and Business Considerations in Choosing IT Services

*Strategically Navigating Technology  
Partnerships for Legal Professionals*



## Mat Kresz

*Attorney at Law*

312-967-5900 (Office)

312-986-9600 (Cell)

MBK@KreszLaw.com

## Brief Background Mat Kresz *Esq.*

- ▶ Mat Kresz is a technology attorney in Chicago. His practice includes a focus on data privacy, cybersecurity, and technology transaction and litigations matters.
- ▶ Prior to law school, Mat served as a business leader and Chief Information Officer (CIO) at a mid-size enterprise that served Fortune 500 clients.
- ▶ Through the business and technology experience he gained in those roles, Mat is equipped to identify opportunities, solve problems, and mitigate risk with business requirements in mind.

# Today's Agenda

1. Legal Ethics at the Intersection of the Practice of Law & IT Operations
2. Role of IT Vendors
3. Vendor Selection Process
4. Managing the IT Vendor Relationship
5. When to Reconsider your IT Vendor

# Why this Presentation Matters to Solo Practitioners

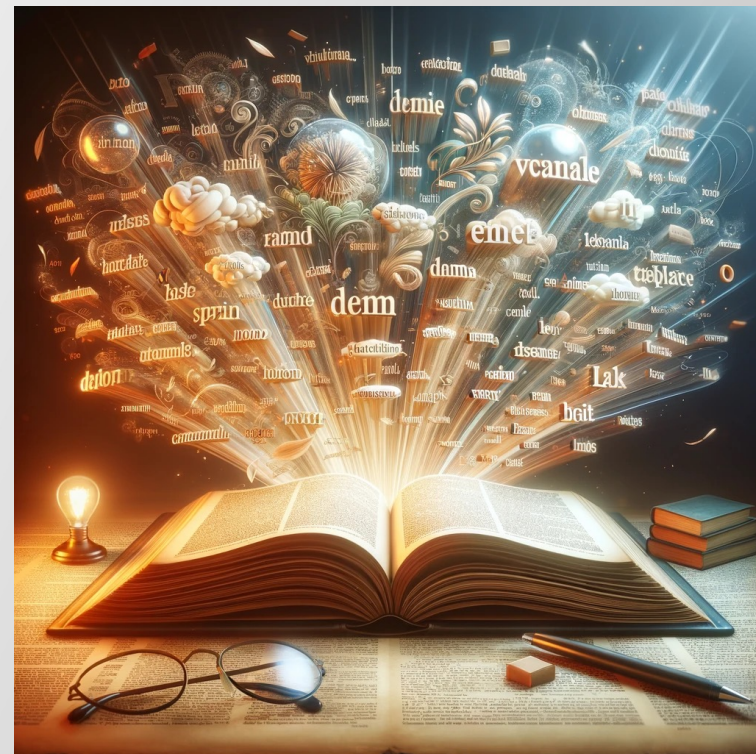
Large firms (and businesses) have ample resources and experience that helps them choose ethical, reliable IT vendors that fit their business needs.

Solos (and small businesses) don't have as much in-house expertise.

**This presentation helps bridge the gap: it will help you select and onboard IT vendors that are better suited for your needs, while meeting your professional ethics obligations.**



# Definitions





# Definitions

## ▶ **Break-Fix Services or Break-Fix Service Provider**

IT services are provided on-demand to fix something that broke, generally on a time-and-materials basis.

## ▶ **MSP or Managed Services**

- ▶ A Managed Service Provider provides “managed IT services” on an on-going basis. The customer usually pays a fixed monthly fee that is based on the number of users and the services that are provided by the MSP.
- ▶ MSPs commonly provide such services as: patch management, network monitoring, data backup and recovery, and Help Desk support.
- ▶ MSPs often re-sell and support third-party products and services such as Microsoft 365 licensing, EDR software, backup and recovery solutions, cloud storage services, and telephony services.

## ▶ **Patch Management**

The process of applying software updates (patches) to information systems to correct security vulnerabilities and improve functionality. (Ex.: Updates of Windows, MacOS, Microsoft Office, Firewall Firmware, Printer Firmware.)

## ▶ **Network Monitoring**

Continuous observation of network components such as routers, switches, firewalls, and servers for issues including service degradation or failure.

## ▶ **End-Point** as in, **End-Point Security**

Any device that connects to a network that communicates with other network devices. This includes computers (desktops, laptops), mobile devices (smartphones, tablets), servers, and other smart devices (IoT devices).

## ▶ **Anti-Virus or Anti-Malware**

Software that identifies a virus or malignant software application based on its apparent characteristics, such as for example its file name or its hash, when those characteristics are matched with the Anti-Virus product’s “definition” file, without particular regard for its behavior.

## ▶ **EDR**

Endpoint Detection and Response. EDR is a cybersecurity technology that monitors endpoints for threats and suspicious activities to uncover advanced attacks.

## ▶ **SLA v. SLO**

Service Level Agreement. An agreed level for service performance.  
Service Level Objective. An aspirational target for service performance.

## ▶ **EOL**

End of Life. Tech (hardware or software) that is no longer supported.

# Definitions

## ▶ **Customer Lock-In** or **Vendor Reliance**

Circumstances that can make it difficult for a customer to change its IT service provider.

## ▶ **Consultant**

A specialist that provides IT services in a niche area. For example, a Cybersecurity Consultant helps clients analyze security risks, develop strategies to mitigate threats, and implement security solutions.

## ▶ **Maturity** as in, **Cybersecurity Maturity**

- ▶ The extent to which an organization has developed and implemented comprehensive cybersecurity protocols and practices, including the depth and sophistication of those practices to protect against cyber threats.
- ▶ A mature cybersecurity posture includes well-established policies, advanced risk management strategies, ongoing employee training, robust incident response plans, and a culture of security awareness. It also implies
- ▶ Continuous improvement and adaptation to new threats in line with industry standards and regulations is implied.

## ▶ **Business Continuity**

The planning that is undertaken by an organization and the processes that are put in place to help ensure that the organization can maintain essential operations and continue to protect assets during a significant disruption.

## ▶ **Disaster Recovery**

The specific plans and technologies an organization uses to recover its IT operations, data, and systems after a disaster or significant disruption.

## ▶ **VAR**

Value Added Reseller. A firm that sells a certain system or solution that also has the expertise to customize it and implement it. VARs often have close relationships with the manufacturers / publishers of the solutions they sell.

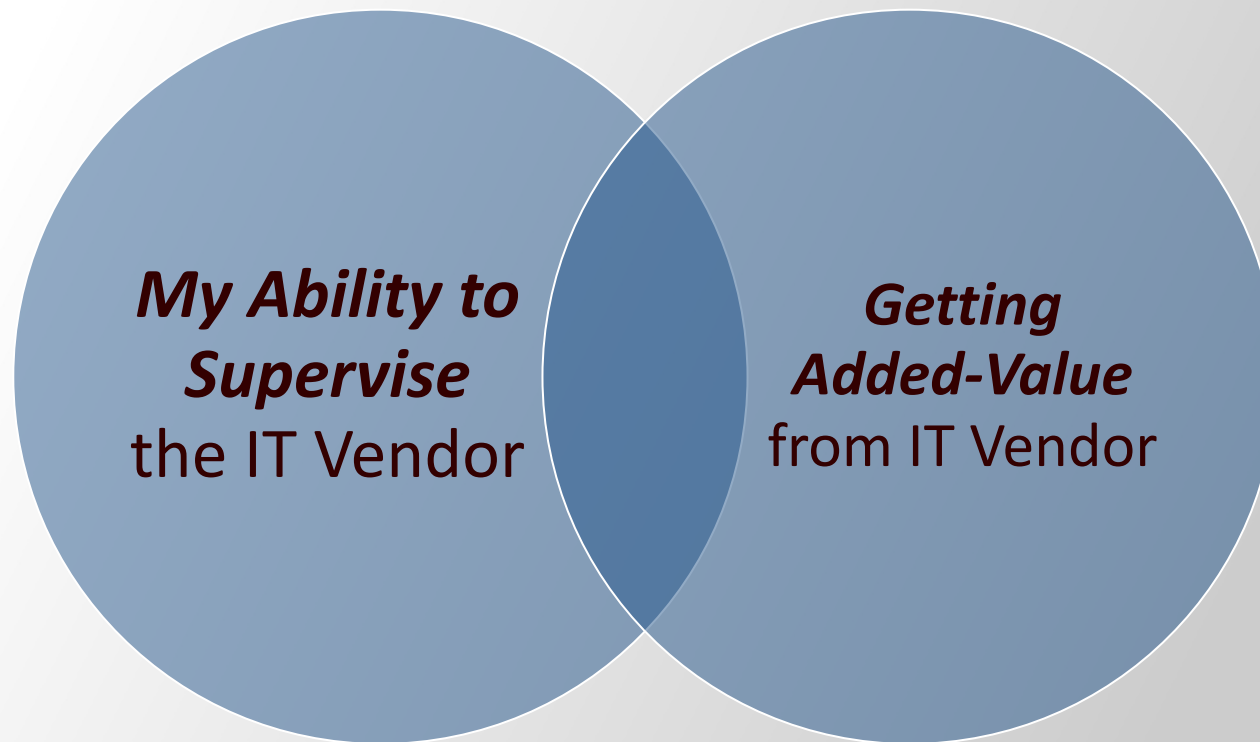
## ▶ **SOC**

Security Operations Center. A centralized unit that continuously monitors and analyzes an organization's security posture on an ongoing basis. The SOC team is responsible for detecting, analyzing, and responding to cybersecurity incidents. The SOC is equipped with sophisticated tools for incident detection and response, such as SIEM (Security Information and Event Management) systems, intrusion detection systems (IDS), and other advanced threat detection technologies.

# Legal Ethics *at the Intersection of the Practice of Law & IT Operations*



# Two Sides to the IT Vendor Relationship

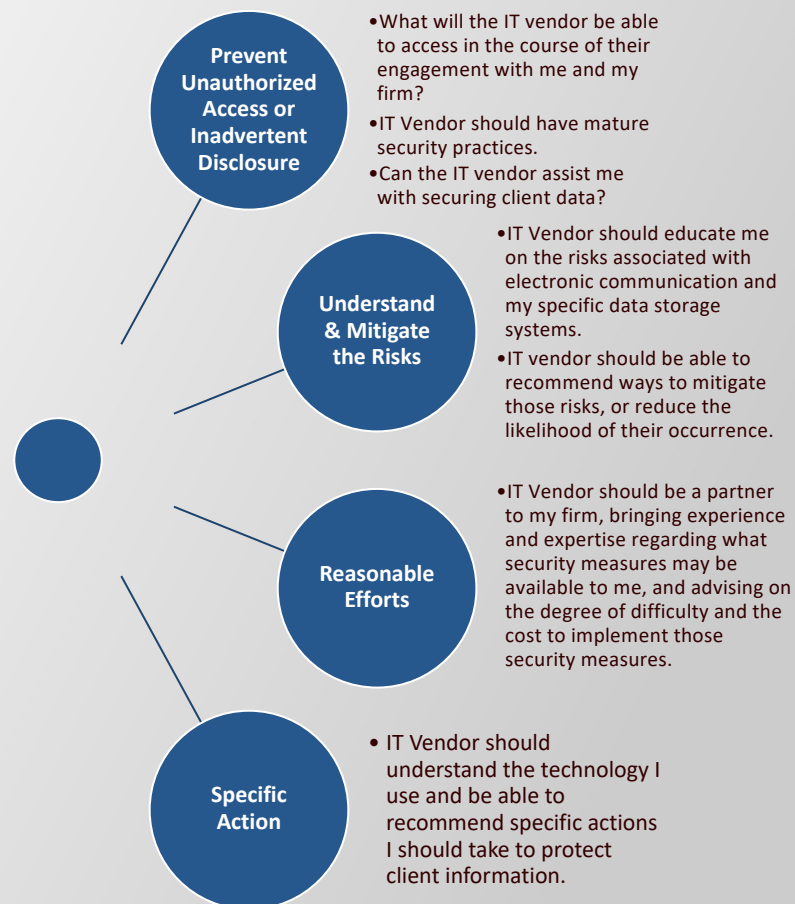


# Nexus Between Ethics & IT Vendors

## ▶ ABA Formal Opinion 477R

### *Securing Communications of Protected Client Information*

- ▶ A lawyer must make reasonable efforts to prevent unauthorized access to or inadvertent disclosure of client information.
- ▶ Attorneys must understand and mitigate the risks associated with electronic communication and data storage.
- ▶ “Reasonable efforts” require a fact-based analysis, considering factors such as the sensitivity of information, potential impact of disclosure, and cost and difficulty of implementing security measures.
- ▶ The specific actions required to protect client information may depend on the nature of the information and the form of technology used.



# Nexus Between Ethics & IT Vendors

## ▶ ABA Formal Opinion 498

### *Virtual Practice*

- ▶ **Competence in Technology Use**  
Attorneys should stay abreast of the technology they use, and understand the tools and platforms used for communication, document storage, and client interactions.
- ▶ **Safeguarding Confidential Information**  
The duty to protect client information from unauthorized access or inadvertent disclosure involves understanding the vulnerabilities associated with electronic communication and data storage, and implementing reasonable security measures.
- ▶ **Vendor Selection and Supervision**  
Attorneys must conduct due diligence to ensure that the vendors' policies and practices comply with ethical standards, particularly regarding confidentiality and security. Lawyers must ensure that contracts or terms of service with vendors do not compromise their ethical obligations to clients.
- ▶ **Notification in Case of a Data Breach**  
Should a data breach occur, attorneys have an ethical obligation to notify clients whose confidential information may have been exposed or compromised.

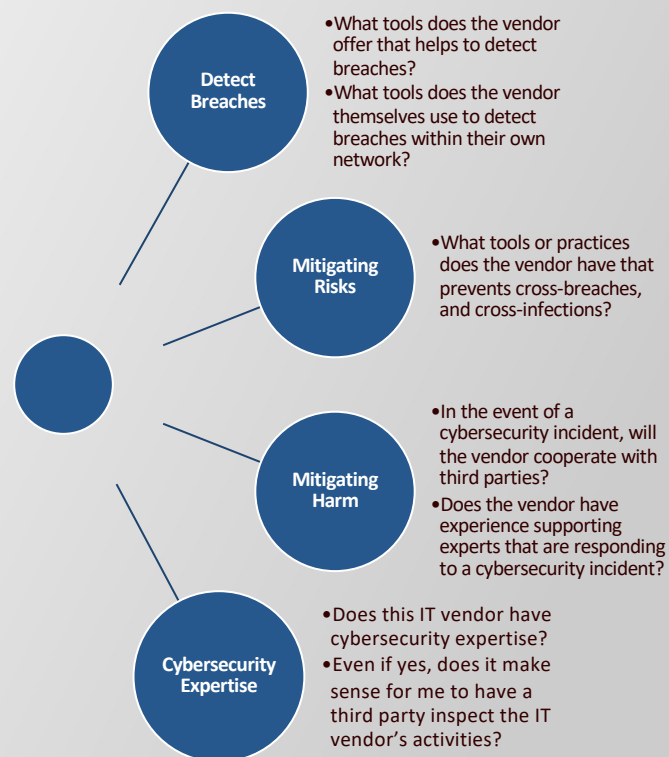


# Nexus Between Ethics & IT Vendors

## ▶ ABA Formal Opinion 483

### *Lawyer's Obligations after Electronic Data Breach or Cyber Attack*

- ▶ In addition to the preventative measures outlined in previous opinions, attorneys have a duty to act competently in detecting breaches, notifying affected clients, and taking steps to mitigate harm.
- ▶ Compliance with ethical responsibilities may require seeking technical advice from cybersecurity experts.
  - ▶ Duty of Competence  
*Model Rule 1.1*
  - ▶ Duty of Confidentiality  
*Model Rule 1.6*
  - ▶ Supervisory Obligations  
*Model Rules 5.1 and 5.3*



## The Role of IT Vendors





# Role of IT Vendors

- ▶ The role of any IT vendor is to support your business operations.
  - ▶ Fix issues (Break-Fix)
  - ▶ Preventative Maintenance (MSP)
  - ▶ Significant Changes (Projects)
  - ▶ Solve Specific Challenges (Consultant)
  - ▶ Advise on Emerging Technologies
  - ▶ Best Practice Use of Current Technology
- ▶ In most cases, IT vendors will have access to your client data.

## The Vendor Selection Process



# Vendor Selection Process



# Vendor Selection Process

## 1. Define Your Requirements

- ▶ Assess your specific needs.
  - ▶ Break-Fix Support? MSP Services? Project Execution? Consulting?
  - ▶ In the simplest terms, what do you want to achieve?
- ▶ Capture your requirements.
  - ▶ Narrative format is OK.
  - ▶ Allows you to compare “apples to apples.”

# Vendor Selection Process

## 2. Request & Evaluate Proposals

- ▶ **Identify Firms** that render the services you need through research, peer recommendations, publications, and professional networks.
- ▶ **Pre-Screen Vendors** based on their service offering & experience.
- ▶ **Draft an RFP** that captures your requirements and your expectations regarding data security, confidentiality, and ethical compliance.
- ▶ **Solicit Proposals** and engage in the vendor's discovery process to help refine your needs and expectations. This is an opportunity for you to inquire about the vendor, too.
- ▶ **Engage In Discovery** to help the vendor understand what you may need.  
Note: Discovery goes both ways. The vendor will want to understand your needs, and you will want to understand their capabilities and their practices.
- ▶ **Evaluate Proposals** asking yourself: did the vendor meet my requirements?  
Do they appear to have the discipline, procedures, processes, and tools to safeguard my clients' data?  
Do I understand the fee structure?

# Vendor Selection Process

## 3. Due Diligence & Vendor Interview

- ▶ Background / Reference Checks
  - ▶ What references can they provide?
  - ▶ Prior involvement in cybersecurity incidents?
  - ▶ Technicians that will be involved day-to-day?
  - ▶ Company's longevity and history?
- ▶ Experience
  - ▶ Does the vendor have experience working with attorneys & law firms?
  - ▶ Are they familiar with an attorneys' obligations?
  - ▶ What clients are not a good fit?
- ▶ Similar Projects
  - ▶ Case studies of similar projects?
- ▶ Degree of Cybersecurity Maturity
  - ▶ How are client systems accessed?
  - ▶ How are client-access credentials protected?
  - ▶ What safeguards are in place to prevent cyber incidents?
  - ▶ What safeguards are in place to prevent cross-infections?
- ▶ Degree of Knowledge
  - ▶ How do technicians stay abreast of new technologies?
  - ▶ How do technicians stay abreast of best practices?

# Vendor Selection Process

## 4. Selection

### ▶ Review the Proposed Service Agreement

- ▶ Is the agreement clear? Or are amendments advisable?
- ▶ Is pricing clear? What's extra? What's included?
- ▶ What SLAs and SLOs are promised?
- ▶ Do Data Security & Confidentiality clauses meet with professional responsibilities?

### ▶ Negotiate Carefully

- ▶ Will unbundling save money? Is it an option?
- ▶ Can the provider really deliver what you need? Or do you sense a gap too big to bridge?

### ▶ Make Your Selection

- ▶ Inform your chosen vendor, and begin onboarding.
- ▶ Notify the other vendors that were not selected.

# Vendor Selection Process

## 5. Onboarding

- ▶ **Vendor Requirements**
  - ▶ What does the vendor require from you?
- ▶ **Downtime**
  - ▶ Will any systems be down during the transition or start of the project?
- ▶ **Schedule**
  - ▶ When will the engagement begin?
  - ▶ When will the onboarding be complete?



# Managing the IT Vendor Relationship



# Trust, but Verify

- ▶ Periodically verify that the vendor is providing the services you purchased.
- ▶ Verify that the vendor stores any client access credentials securely.
- ▶ Verify that the vendor accesses your systems in a secure fashion.

# Relationship Management

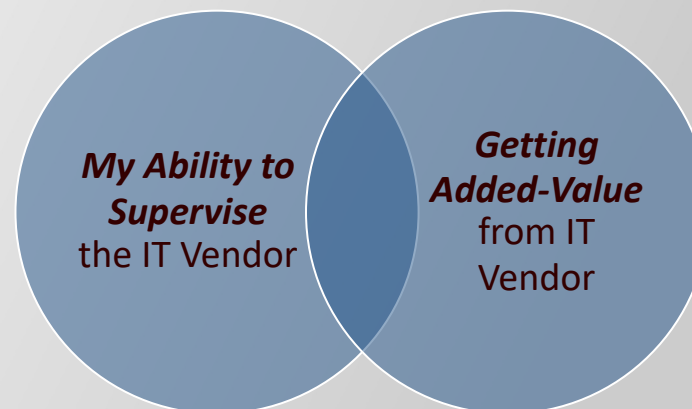
- ▶ Quarterly Meetings or reports
  - ▶ KPIs (Key Performance Indicators) on SLAs
  - ▶ Work Performed
  - ▶ Objectives Achieved
  - ▶ Cybersecurity Instances detected on your domain, as well as theirs.
  - ▶ Opportunities in technology updates, upgrades, education communication.
  - ▶ Forecast discussing End of Life systems, expanded needs, expanded capabilities, emerging technologies.

## When to Reconsider your IT Vendor



# When to Reconsider Your IT Vendor

- ▶ 1. You can't get straight answers or explanations, you're kept in the dark, and you're bamboozled by technical jargon that you don't understand.
- ▶ 2. You don't know what your service provider is actually doing for you.
  - ▶ Note: Do not confuse lack of service issues with lack of services. There were service failures, and the service provider did not explain why, or provide a service remediation plan.
- ▶ 3. Your firm outgrew your service provider, or your service provider outgrew your firm.
- ▶ 4. It's just not working.



# Switching Service Providers

1. Understand what your current vendor can access.
2. Determine if the offboarding is partial or complete.
3. If you are moving to a new vendor, have a clear understanding of their timeline, plan, and requirements.
4. See the transition through.

# Questions & Discussion



**Mat Kresz**

*Attorney at Law*

312-967-5900 (Office)

312-986-9600 (Cell)

[MBK@KreszLaw.com](mailto:MBK@KreszLaw.com)



Get my vCard



**Thank you for  
attending!**







	Other: _____ Service Name? Sell? Migration? Implementation? Support?
Data Backup & Disaster Recovery	Data Backup Solutions? (Yes / No) Comments: _____  Data Recovery Solutions? (Yes / No) Comments: _____  Disaster Recovery Solutions? (Yes / No) Comments: _____
Consulting & Strategy	Long Term IT Strategy & Planning (Yes / No) Comments: _____  Risk Identification (Yes / No) Formal Risk Assessments (Yes / No) Comments: _____  Cyber Security Training? (Yes / No) Comments: _____  Comments: _____
Other: _____	Comments: _____

**2. Proposal Review**

Is the Vendor's proposal clear to me, without technical jargon? ( Yes / No)  
 Questions I have: \_\_\_\_\_

Is the proposal responsive to my specific needs? ( Yes / No)  
 Needs Met / Not Met: \_\_\_\_\_  
 Questions I have: \_\_\_\_\_

What additional services did the vendor propose (beyond my inquiry)?  
 \_\_\_\_\_



Additional services proposed:

Questions I have:

---

Is the pricing structure clear? ( Yes / No)

Questions I have:

---

### **3. Vendor Credentials & Security Practices**

Did the Vendor show relevant experience working with law firms? (Yes / No)

Does the Vendor follow security best-practices, and have its own internal robust security policies? (Yes / No)

Does the Vendor carefully vet their employees? (Yes / No)

Does the Vendor have change-management procedures, including documentation? (Yes / No)

Does the Vendor create their own, unique Admin account on client systems, without re-using the user name and password? (Yes / No)

Does the vendor have its own internal access control policies and internal intrusion detection systems to prevent cross-infections? (Yes / No)

### **4. Fit to Firm's Needs**

Does the Vendor appear to fit my Firm's immediate needs? (Yes / No)

Does the Vendor appear to fit my long-term needs? (Yes / No)

Is there a risk that I will out-grow the Vendor, or that the Vendor will out-grow me? (Yes / No)

### **5. Compliance with Professional Responsibilities**

Does the Vendor have a clear understanding of my professional and ethical duties with regard to keeping client information and client communications confidential and securely protected? (Yes / No)



Does the Vendor understand that they are an integral part in my ability to adhere to my professional duties, and that their failure to maintain good security practices could harm my Firm or my clients? (Yes / No)

#### **6. Customer Service**

Will the Vendor meet with me quarterly to provide and discuss their performance metrics or list of tasks completed? (Yes / No)

Does the Vendor have an escalation process to ensure that I receive service in case of an emergency? (Yes / No)

#### **7. Special Considerations for Security**

Does the vendor have robust internal security practices? (Yes/No)

Do they avoid duplicating access credentials across clients? (Yes/No)

Do they employ two-factor authentication (2FA) in customer environments and in their own internal environment? (Yes / No)

Do they avoid leaving “back doors” in customer environments and in their own internal environment? (Yes / No)

#### **8. Overall Assessment**

Overall Assessment: \_\_\_\_\_

Strengths: \_\_\_\_\_

Weaknesses / Areas of Improvement: \_\_\_\_\_